UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 4:14-CR-122 CEJ NAB
	)	
DAVID SHEN,	)	
	)	
Defendant.	)	
	)	

REPORT AND RECOMMENDATION OF MAGISTRATE JUDGE

The above matter was referred to the undersigned United States Magistrate Judge pursuant to 28 U.S.C. § 636(b). Defendant David Shen was charged by indictment with one count of unauthorized access of a computer and one count of attempted unauthorized access of a computer in violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. [Doc. #2.] Defendant was also charged with a third count for fraud in violation of 18 U.S.C. § 1343 and 2. On February 23, 2015, Defendant filed a Motion to Dismiss Counts I and II of the Indictment. [Doc. #30.] The Government filed its Response on March 2, 2015. [Doc. #32.] On March 25, 2015, the undersigned held a hearing. At the hearing, counsel for Defendant withdrew his motion as to Count II. Having considered the briefs of the parties and argument by counsel at the hearing, the undersigned finds that Defendant's motion to dismiss Count I should be denied.

DISCUSSION

An indictment is sufficient if: (1) it contains all of the essential elements of the offense charged; (2) it fairly informs the defendant of the charges against which he must defend; and (3) it alleges sufficient information to allow a defendant to plead a conviction or acquittal as a

bar to a subsequent prosecution. *United States v. Fleming*, 8 F.3d 1264, 1265 (8th Cir. 1993). "An indictment is normally sufficient if its language tracks the statutory language." *United States v. Sewell*, 513 F.3d 820, 821 (8th Cir. 2008). An indictment is insufficient if it is "so defective that it cannot be said, by any reasonable construction, to charge the offense for which the defendant was convicted." *Fleming*, 8 F.3d at 1265. When a defendant moves to dismiss a count for failure to state an offense, the court takes the allegations in the indictment as true and should refrain from considering evidence outside the indictment. *United States v. Sampson*, 371 U.S. 75, 78–79, 83 S.Ct. 173, 174–75, 9 L.Ed.2d 136 (1962); *United States v. Hall*, 20 F.3d 1084, 1087 (10th Cir. 1994).

Count I of the indictment charges Shen with unauthorized access of a computer in violation of § 1030(a)(2)(C) of the CFAA. Section 1030(a)(2)(C) provides in relevant part: "Whoever … intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer … shall be punished." Through his employment as a risk manager with Washington University, Shen gained access to password-protected third party service providers described in the indictment as Service Provider A and Service Provider B. On October 6, 2011, Shen resigned from his position in lieu of being terminated. Count I charges in relevant part:

> On or about October 28, 2011, in the Eastern District of Missouri and elsewhere, DAVID SHEN, the defendant herein, intentionally accessed a protected computer used in interstate and foreign commerce, without authorization and exceeding any authorized access he had previously been given, and thereby obtained information from that protected computer … to wit, the defendant used his personal computer to access without authorization, and in excess of any authorized access, a computer system associated with Service Provider A and thereby downloaded a Risk Report for Washington University HF Portfolio for the month of August 2011.

[Doc. #2 ¶ 11.] Shen argues that Count I should be dismissed for failure to state an offense because he was authorized to access Service Provider A, either because he used his personal computer or because his password still worked. The undersigned disagrees.

The language of Count I tracks the language of § 1030(a)(2)(C) and the Eighth Circuit Model Jury Instruction.[1] Shen's arguments are essentially challenges to the sufficiency of the evidence, which cannot be decided at this stage. *United States v. Ferro*, 252 F.3d 964, 967-68 (8th Cir. 2001); *United States v. Perez*, 575 F.3d 164, 166-67 (2d Cir. 2009). The indictment reflects that Shen was given access to Service Provider A in connection with his employment and that he accessed Service Provider A after he had resigned. There is significant authority that such access is unauthorized under § 1030(a)(2)(C). *See, e.g., United States v. Steele*, No. 13-4567, 2014 WL 7331679 (4th Cir. Dec. 24, 2014); *cf. United States v. Teague*, 646 F.3d 1119 (8th Cir. 2011).

Furthermore, the fact that Shen used his personal computer does not foreclose a finding of unauthorized access. Count I specifically alleges that Shen accessed "without authorization, and in excess of any authorized access, *a computer system* associated with Service Provider A." While the Government will have to show that Service Provider A's computer system meets the statutory definition of a "computer," nothing more is required at this stage. *Cf. Keystone Fruit Mktg., Inc. v. Brownfield*, No. CV-05-5087-RHW, 2006 WL 1873800, at *6 (E.D. Wash. July 6,

[1] Model Instruction 6.18.1030B provides in relevant part:

> The crime of computer fraud to obtain confidential information … has two essential elements, which are:
>
> *One*, the defendant intentionally accessed a computer without authorization or exceeding authorized access, and
>
> *Two*, the defendant obtained information.

2006) (deciding similar issue on summary judgment in case involving civil § 1030(a)(2)(C) claim).

Shen additionally argues that § 1030(a)(2)(C) is impermissibly vague as applied to him. He essentially argues that his authorization hinges on an agreement between his employer and Service Provider A which he never saw and therefore he had no notice that his conduct was criminal. The argument fails. There is some disagreement as to whether an employee who properly accesses a computer and then misuses the information can be convicted under § 1030(a)(2)(C). *See United States v. Nosal*, 676 F.3d 854, 862 (9th Cir. 2012). However, courts are clear that employees who gain access to a computer through their employment lose authorization once they have resigned or been terminated. *See, e.g., United States v. Steele*, No. 13-4567, 2014 WL 7331679 (4th Cir. Dec. 24, 2014); *cf. United States v. Teague*, 646 F.3d 1119 (8th Cir. 2011). Moreover, persons of common intelligence would understand as much.

For the foregoing reasons, the undersigned recommends that Shen's motion to dismiss Count I be denied.

ACCORDINGLY,

IT IS HEREBY RECOMMENDED that Defendant's motion to dismiss Count I [Doc. #30] should be **DENIED.**

The parties are advised that they have fourteen (14) days in which to filed written objections to this report and recommendation pursuant to 28 U.S.C. § 636(b)(1). Failure to timely file objections may result in a waiver of the right to appeal questions of fact.

Dated this 21st day of April, 2015.

/s/ Nannette A. Baker
NANNETTE A. BAKER
UNITED STATES MAGISTRATE JUDGE